



OPSEC and Social Networking



Naval OPSEC Support Team (NOST)
Navy Information Operations Command (NIOC)
(757) 417-7100 DSN 537
OPSEC@navy.mil
www.facebook.com/NavalOPSEC
www.twitter.com/NavalOPSEC
www.slideshare.net/NavalOPSEC

UNCLASSIFIED



References



- DTM 2009-026 Responsible & Effective use of Internet-based Capabilities
- SECNAVINST 5720.47B DON WWW Web Policy
- DON CIO_CHINFO Joint Memo 10_Oct 07_DOC Web Presence Policy
- NTTP 3-54 M Operations Security
- DOD Directive 5205.2 OPSEC Program
- OPNAVINST 3432.1 Operations Security
- DON Navy Public Affairs Policy & Regulations SECNAV 5720.44B
- DON Policy for Content of Publicly Accessible World Wide Web Sites SECNAV 5720.47B
- <http://www.chinfo.navy.mil/socialmedia.html>
- COMNAVREGMIDLANTINST 5720.1 Web 2.0 Technologies
- <http://www.iooss.gov/> Social Networking Sites Safety Checklist
- ALNAV 056-10 IbC- Official Internet Posts
- ALNAV 057-10 IbC- Unofficial Internet Posts

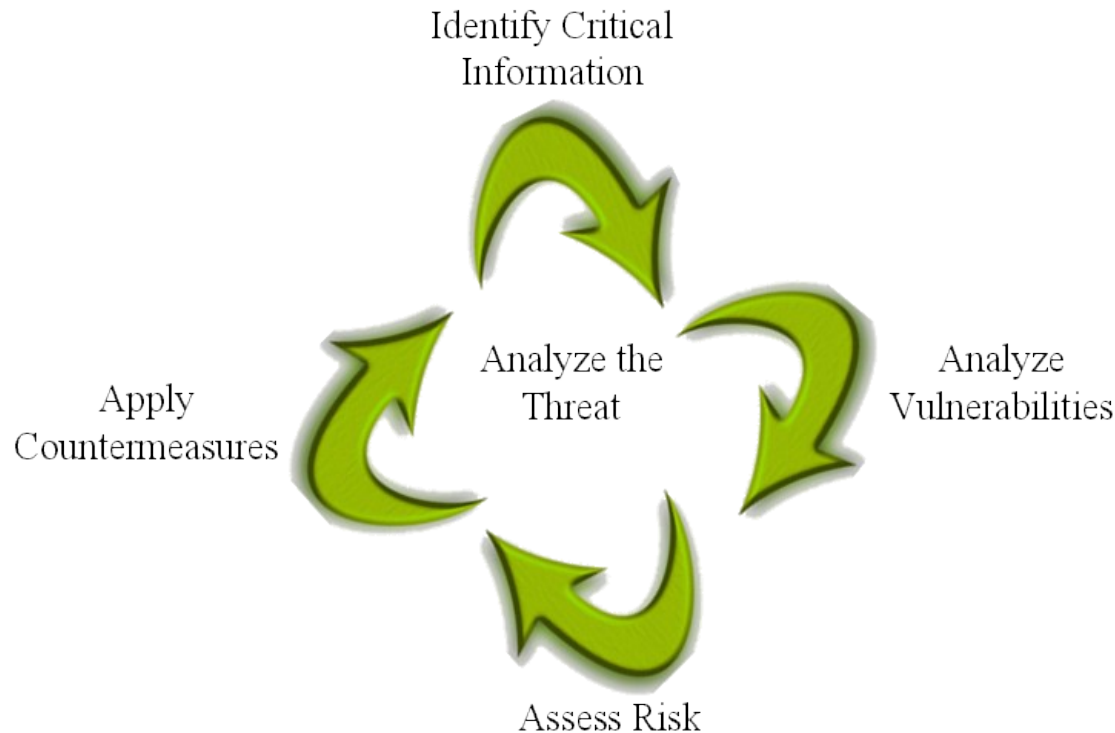
UNCLASSIFIED



Operations Security OPSEC



OPSEC is a process that identifies critical information, outlines potential threats and risks and develops counter measures to safeguard critical information



UNCLASSIFIED



Critical Information



- Information **we must protect** to ensure success
- Information the **adversary needs** to prevent our success.

- Names and photos of you, your family and co-workers
- Usernames, passwords, network details
- Job title, location, salary, clearances
- Physical security and logistics
- Position, mission capabilities and limitations
- Operations & missions
- Schedules and travel itineraries
- Social security number, credit cards, banking information
- Hobbies, likes, dislikes etc.

UNCLASSIFIED





Data Aggregation

- Information collection from multiple sources
- Al Qaeda handbook: open and legal public sources accounts for 80% of all information collected
- Legal and illegal collection methods



UNCLASSIFIED

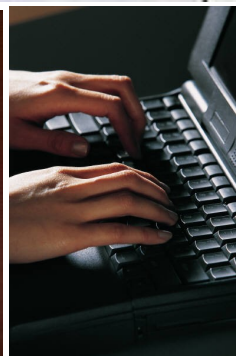


Potential Vulnerabilities



Methods used to obtain Critical Information:

- Unprotected communications
- Sharing too much with strangers
- HUMINT Observation
- Technology
- Trash
- Media
- Email
- Web pages
- Social Networking Sites



Illegal methods are OK with adversaries!!!

UNCLASSIFIED



Social Networking

Social Networking Sites (SNS) allow people to network, interact and collaborate to share information, data and ideas without geographic boundaries.

GoogleTM
Social

☺ friendster.

foursquare



orkut

hi5



BloggerTM



netvibes



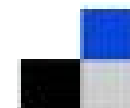
Fröpper

You Tube

Broadcast Yourself

Linked in

YAHOO! 360°
BETA



del.icio.us

UNCLASSIFIED



Revised Statement of Rights & Responsibilities



- “You own all of the content & information you post.”
- “You specifically give us the following permission,
subject to your privacy and application settings to

Consent to Collection and Processing in the United States. By using Facebook, you consent to having your personal data transferred to and processed in the United States.

- “We may collect information about you from other users.”
- “Sometimes we share aggregated information with third parties.”

UNCLASSIFIED



Why use a SNS?

Personally

- Entertaining
- Maintain Relationships
- Network
- Centralized information

Professionally

- Marketing/recruiting
- Public Relations
- Connect with customers
- Solicit ideas and feedback



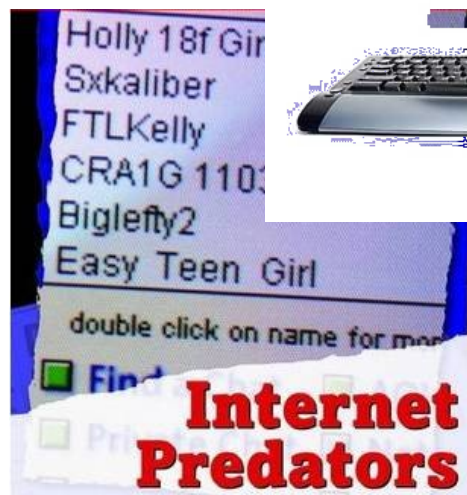


The Danger



Bad guys use it, too:

- Stalkers
- Thieves
- Terrorist
- Hackers
- Phishers/Scammers
- Enemy organizations
- Pedophiles
- And the list goes on...



UNCLASSIFIED



The Danger

Al-Qaeda communiqué December 2009:



“The affair with the U.S. Navy began several years ago, when the lions of Al-Qaeda struck the destroyer U.S.S. Cole, in Yemen; now, with Allah’s help, all the American vessels in the seas and oceans, including aircraft carriers, submarines, and all

Information on every U.S. Naval unit should be quietly gathered...what state they are from, their **family** situation, and where their **family** members live...

...search for the easiest ways of striking these ships...

.... Do not underestimate the importance of any piece of information, as simple as it may seem....

UNCLASSIFIED



Social Networking Websites and Your Security Clearance



The following is a security awareness statement signed by the

Question 14 of the National Agency Questionnaire (SF-86) asks for **names of your relatives and associates. The term associate is defined as any foreign national that you or your spouse are bound by affection,**

obligation, or close and continuing contact.

86) asks for names of your relatives and associates. The term associate is defined as any foreign national that you or your spouse are bound by affection, obligation, or close and continuing contact.

UNCLASSIFIED



DO'S & DON'TS of SOCIAL NETWORKING

UNCLASSIFIED



“Do’s”



Do: Remember Computer Security

Do not be an easy target for computer crimes

- Hacking
 - Theft
 - Planted code
- vs.
- Antivirus software
 - Firewalls
 - Strong Passwords
 - Permission Settings



UNCLASSIFIED



“Do’s”



Do: Verify All Friend Requests

Social engineering and “conning” starts with a friend request



Adversaries can get the data from

- Free people search engines
- Other SNS's
- Your posts/profile
- Your friends posts/profile

Verify Requests Before Approving

UNCLASSIFIED

Adversary



“Do’s”

Do: Utilize All Available Privacy Settings

Customize available settings to be as secure as possible

- “Everyone” may be accessed by anyone with access to the internet

- How many security settings are available

Over 120

UNCLASSIFIED





“Do’s”



Do: Watch Your Friends Settings

Sure your profile is secure, but what about your 115 friends profile settings?



UNCLASSIFIED

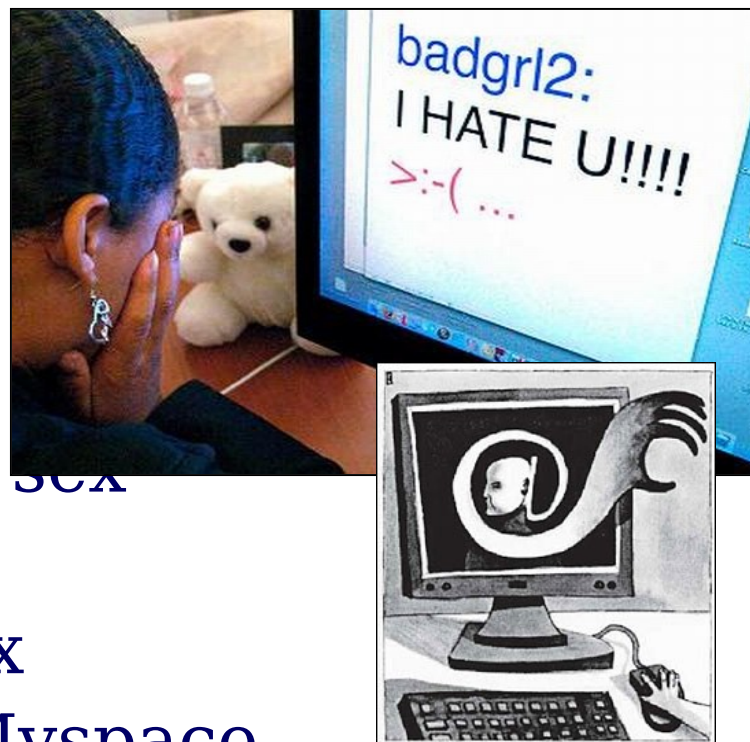


“Do’s”



Do: Closely Monitor Your Children’s Use of the Internet

- Cyber-bulling
- Kidnapping
- “Sexting”
- Stalking
- Pedophiles
 - 500,000+ registered sex Offenders in the USA
 - 95,000 registered sex offenders profiles on Myspace



UNCLASSIFIED



"Do's"



Do: Verify Links & Files Before Executing

Would you follow a link in e-mail? Would you download and run an attachment? Then why do you do these things on SNS's?

- Phishing scams
- Malicious coding
- Viruses
- Scareware

Verify before execut



UNCLASSIFIED

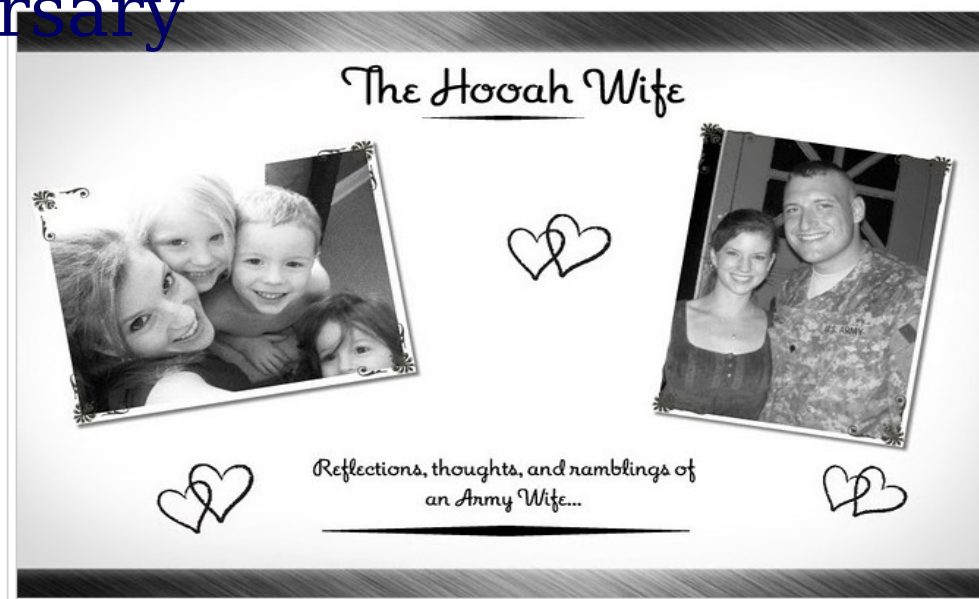


“Do’s”



Do: Blog with Caution

- Avoid details, don't get personal
- Who is reading your blog?
- Lessons learned 101 for the adversary



UNCLASSIFIED



“Do’s”



Do: Understand the Risks Associated with Geotagging

- Location/GPS data attached to photos
- Feature in Smartphones and digital
 - Lat/Long
 - Device details
- “Check-in” feature
 - Facebook Places
 - Google Latitude
 - Foursquare
 - Gowalla



UNCLASSIFIED



“Do’s”



Do: Be an Informed User of a SNS

- How much personal information do you broadcast?
- Are you very careful about what details you post?
- Do you understand data aggregation issues?
- Are you willing to find and learn all the security settings and keep up with them as they change?



Are you willing to accept the risk?

UNCLASSIFIED



“Do’s”



Do: Have a Contingency Plan

- KIA, MIA, POW
- What details will the adversary have to use against you?
- What information will the media have access to?
- Power of Attorney
- Memorial pages



UNCLASSIFIED



“Do’s”



Do: Assume the Internet is FOREVER

- There is no true delete on the internet
- WWW means World Wide Web
- Every Picture
- Every Post
- Every Detail

forever



“Do’s”



Do: Understand Official DON Guidance That Governs Military Personnel Use of SNS's

- DON ALNAV 056/10 Official Internet Posts
 - Social media posts in an official capacity
- DON ALNAV 057/10 Unofficial Internet Posts
 - Any content posted about the DON by DON personnel in an unofficial & personal capacity
 - DON personnel are responsible for all DON^r related content they publish on the internet



UNCLASSIFIED



“Don’ts”



Don’t: Use the Same Passwords

- Hackers count on users using the same passwords for multiple accounts
- Password1 is not a strong password

Password:

Strength: Weak

flickr - ianwalth - password



"Don'ts"



Don't: Depend on SNS's Security Settings

But it's set to private ... right?

- Hackers
- Incorrect or incomplete settings
- Sale of data
- Upgrades/site changes
- "Risks inherent in sharing information"
- "USE AT YOUR OWN RISK. We do not guarantee that only authorized persons will view your information."



UNCLASSIFIED



“Don’ts”

Don’t: Trust Add-On’s or Applications

- Plugins, Games, Applications
 - Third Party Software
 - Applications designed to collect data
 - Malicious code
 - Separate terms of use & privacy
 - “We are not responsible for third party collection of your information or any other measures.”



UNCLASSIFIED



“Don’ts”



Don’t: Grant the Same Access to Everyone

- Don’t treat all Friends equally
- Control & customize individual access
- Do create groups
 - Poker club
 - Family
- Set permissions for everything
 - Your status
 - Photos
 - Postings

A screenshot of a Facebook profile's privacy settings page. The page is divided into two main sections. The left section lists various profile elements with their current privacy settings. The right section shows a list of these settings with corresponding dropdown menus to change them. The settings listed on the left are: About me (About Me refers to the About Me description in your profile), Personal Info (Interests, Activities, Favorites), Birthday (Birth date and Year), Religious and Political Views, Family and Relationship (Family Members, Relationship Status, Interests), Education and Work (Schools, Colleges and Workplaces), Photos and Videos of Me (Photos and Videos you've been tagged in), Photo Albums, and Posts by Me (Default setting for Status Updates, Links, and Photos). The right section shows dropdown menus for each of these settings, with most set to "Only Friends" and one set to "Only Me". At the bottom of the right section is an "Edit Settings" button.

UNCLASSIFIED



"Don'ts"



Don't: Discuss Details

- Never post anything you would not tell directly to the end user
- Never post private or personal information- no matter how secure you think your settings are
- Assume the information you post will be made public



Details make you vulnerable

UNCLASSIFIED



Questions?



Please contact the NOST for assistance or any of the following:

- Computer-based training
- FRG/Ombudsman support
- OPSEC & other tailored briefs
- Videos , posters, brochures & fliers
- OPSEC Reminder Cards
- Two-day Navy OPSEC Officer course
- General OPSEC support
- Other Resources

Countries don't have friends...



They have interests. Which country is interested in what you do?

Naval OPSEC Support Team

opsec@navy.mil

757-417-7100

www.facebook.com/NavalOPSEC

www.twitter.com/NavalOPSEC

www.slideshare.net/NavalOPSEC

UNCLASSIFIED